

The diagram illustrates a cryptographic system 108. It begins with an **INPUT** block (64) labeled 110, which feeds into an **INITIAL PERMUTATION** block (112). The output of the initial permutation is split into two paths: one leading to block 114 and another to block 116. Block 114 is labeled **PERMUTED INPUT** and contains a block L_0 . Block 116 contains a block R_0 . A key block K_1 (118) is connected to the R_0 path. The outputs of L_0 and R_0 are combined in a block 120, which includes an addition (+) and a function f . The output of block 120 is then split into two paths: one leading to block $L_1 = R_0$ and another to block $R_1 = L_0 + f(R_0, K_1)$. This process repeats for subsequent rounds, with blocks $L_2 = R_1$ and $R_2 = L_1 + f(R_1, K_2)$ shown. A dashed line indicates a continuation of this process through blocks $L_n = R_{n-1}$ and $R_n = L_{n-1} + f(R_{n-1}, K_n)$. The final round shown is $L_{15} = R_{14}$ and $R_{15} = L_{14} + f(R_{14}, K_{16})$. The output of this round is split into two paths: one leading to block $R_{16} = L_{15} + f(R_{15}, K_{16})$ and another to block $L_{16} = R_{15}$. These two paths are combined in a block 126, which is labeled **PRE-OUTPUT**. The output of block 126 then feeds into an **INVERSE INITIAL PERM.** block (130). The final output is an **OUTPUT** block (64) labeled 132.

108

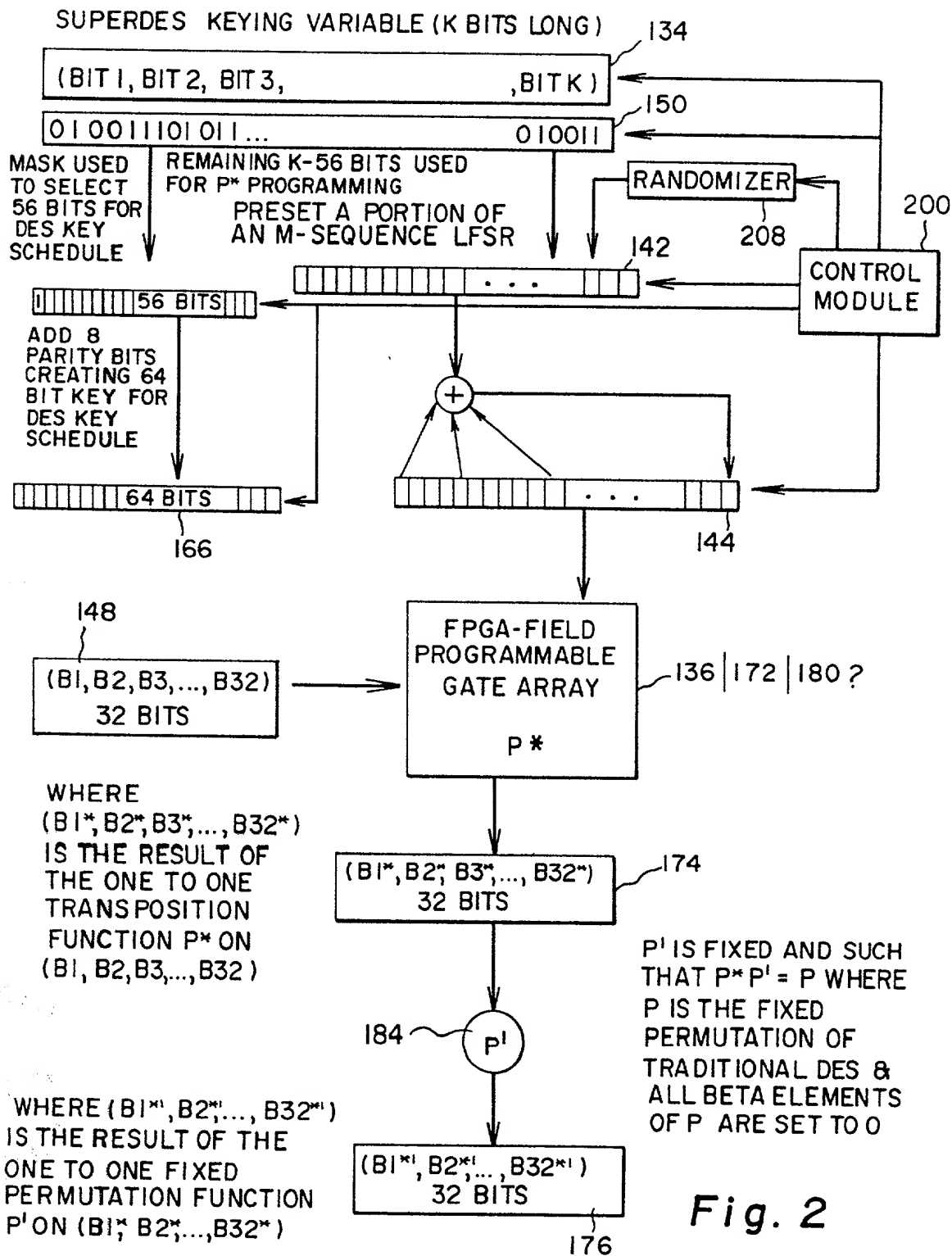


Fig. 2

120

0933163-03301

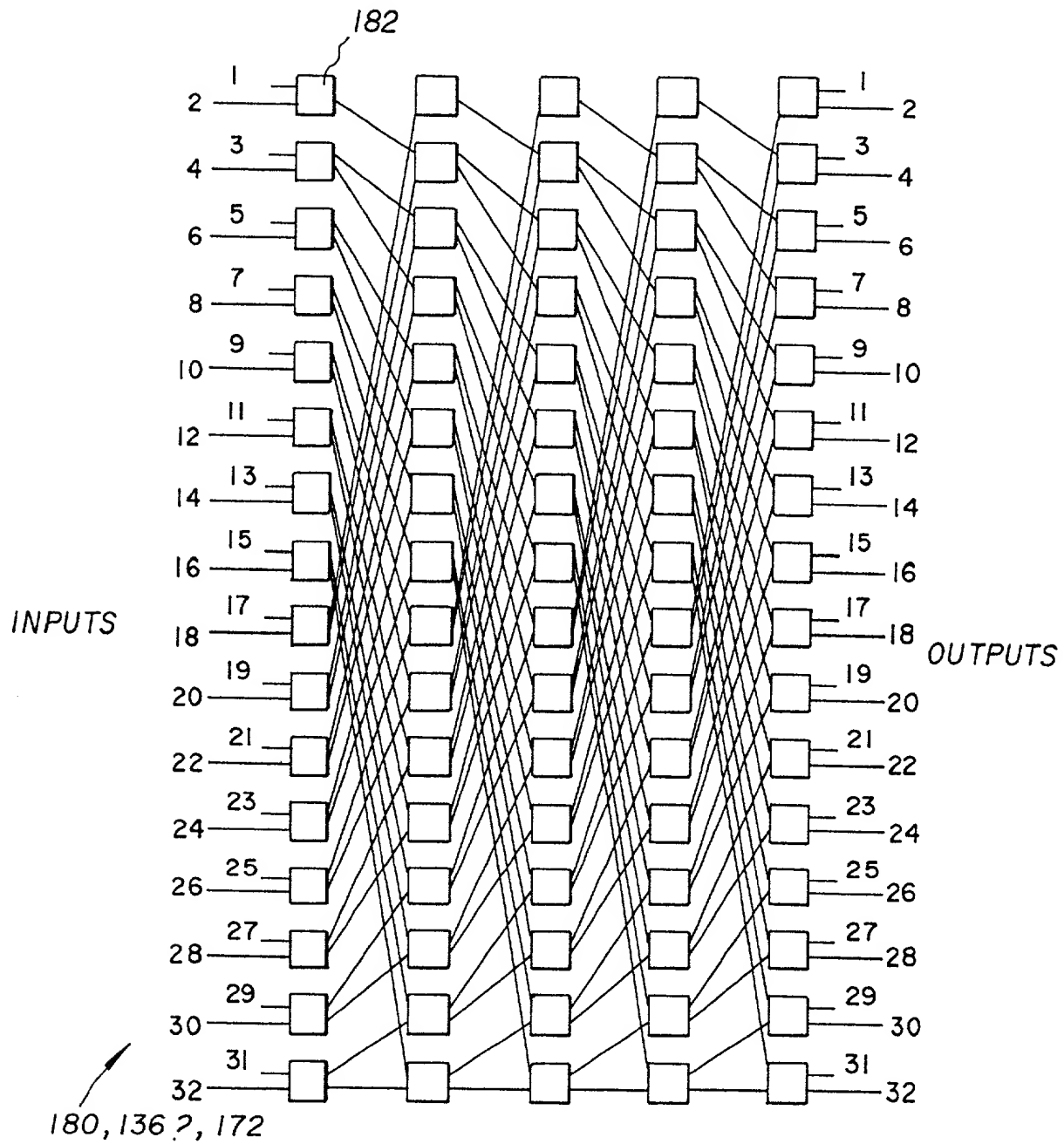


Fig. 4

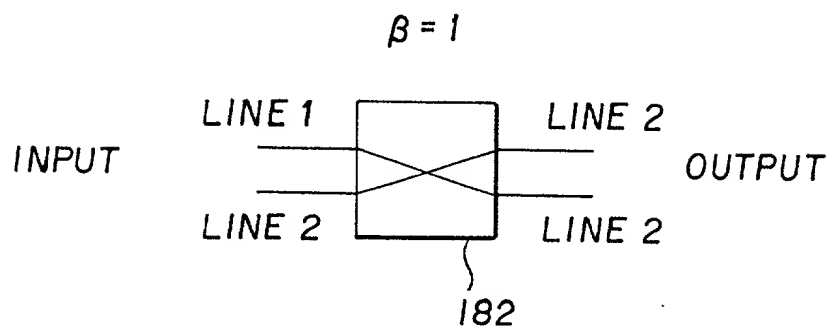
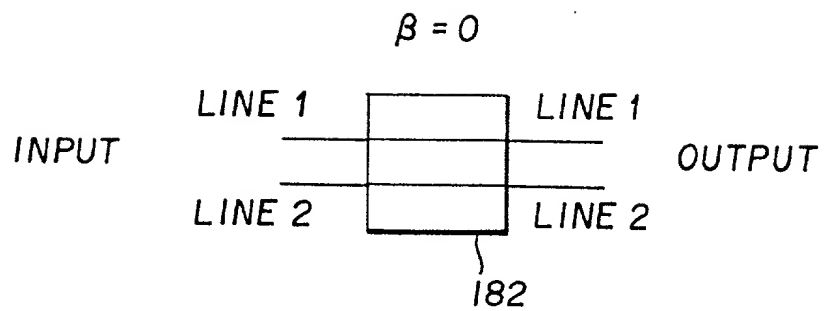


Fig. 5

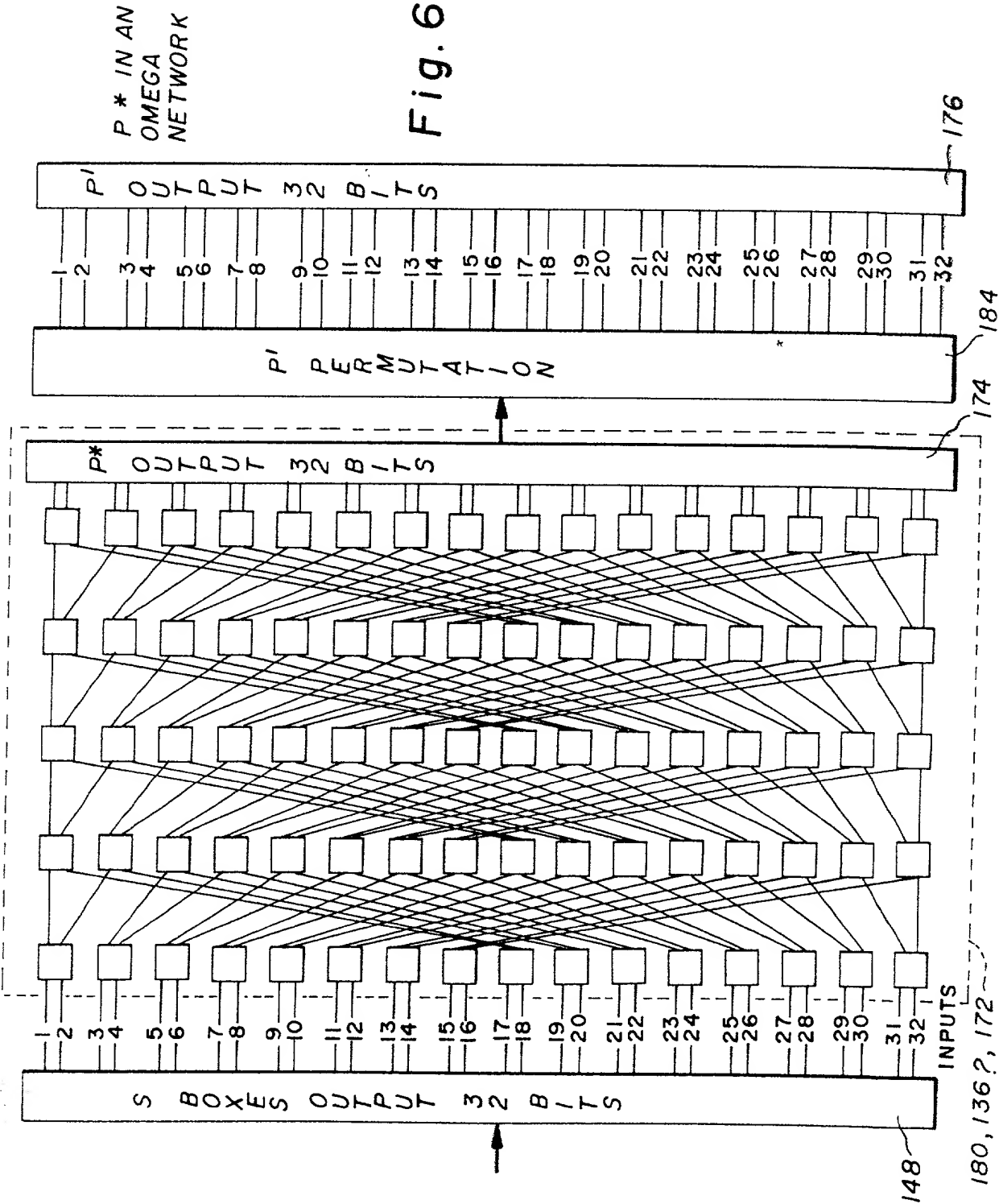


Fig. 6

P* IN AN
OMEGA
NETWORK

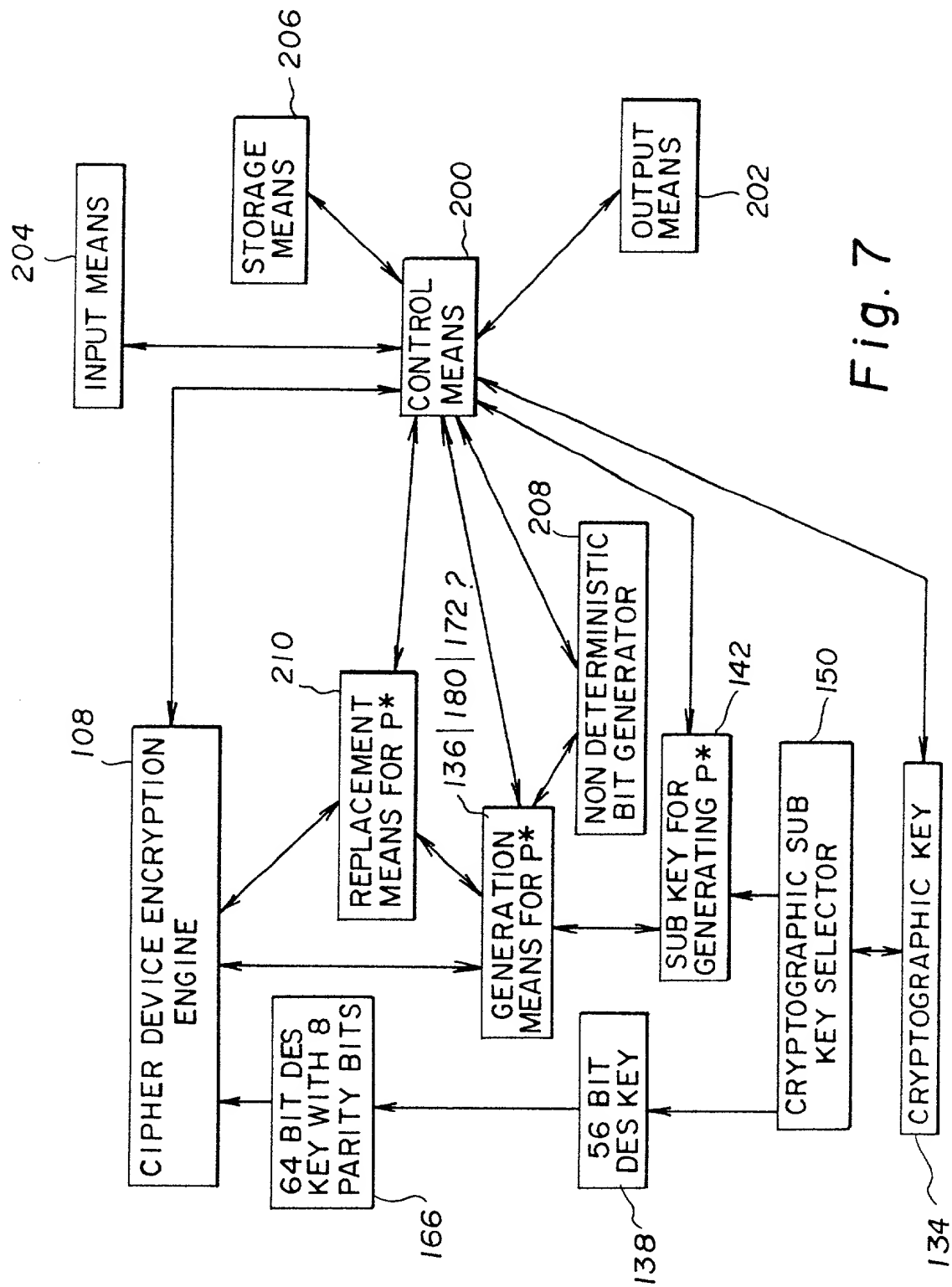


Fig. 7

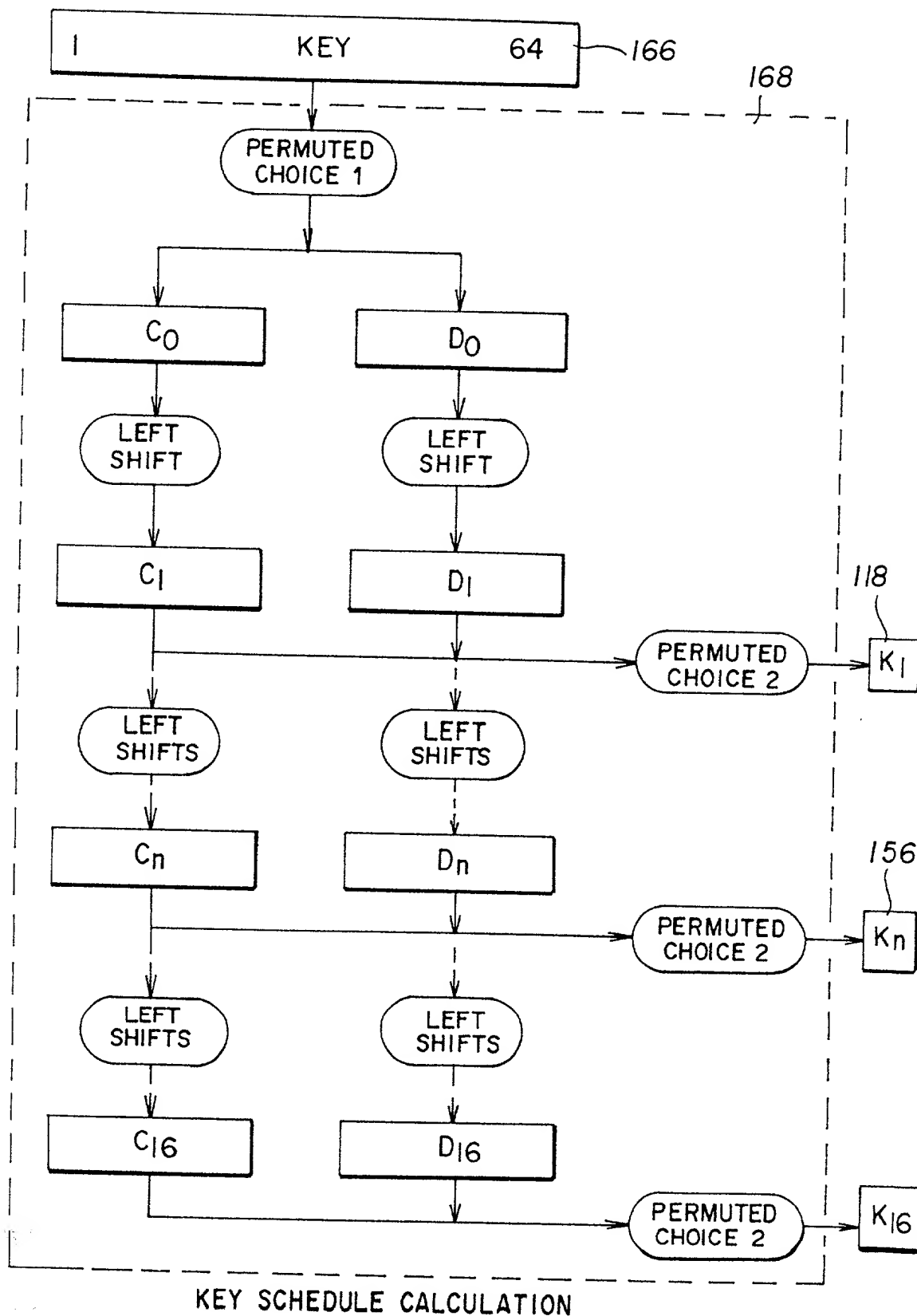


Fig. 8